

65918 U.S. PTO  
07/28/97

THE COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, DC 20231

Attorney Docket: JAS 545P  
PATENT

Sir:

Transmitted herewith for filing is the Patent Application of

Inventor: **John Philip Pettitt**

For: **A METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT CARD  
TRANSACTION OVER THE INTERNET**

Enclosed with the Patent Application are:

- ☒ Four (4) sheets of informal drawings
- ☒ Declaration of Inventor(s)
- ☒ Power of Attorney by Assignee
- ☒ Declaration Claiming Small Entity Status
- ☒ Assignment and Recordation Form
- ☐ Information Disclosure Statement (PTO Form 1449)
- ☐ A certified copy of a \_\_\_\_\_ application.
- ☒ Self Addressed, Stamped Postcard

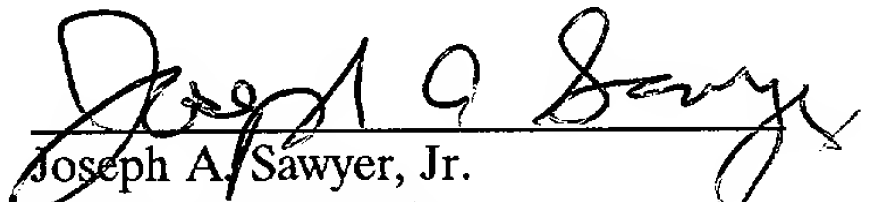
The filing fee has been calculated as shown below:

|   |  | (Col. 1)  | (Col. 2)  | SMALL ENTITY |           |
|---|--|-----------|-----------|--------------|-----------|
| FOR:  |  | NO. FILED | NO. EXTRA | RATE         | FEE       |
| BASIC FEE   |  |           |           |              | \$ 385.00 |
| TOTAL CLAIMS  |  | 16 - 20   | = 0       | x 11 =       | \$ 0.00   |
| INDEP. CLAIMS   |  | 6 - 3     | = 3       | x 40 =       | \$ 120.00 |
| __ MULTIPLE DEPENDENT CLAIM PRESENTED                                 |  |           |           | +125 =       | \$ 0      |
| *If the difference in Col. 1 is less than "0",<br>enter "0" in Col. 2 |  |           |           | TOTAL        | \$ 505.00 |

☒ The Commissioner is hereby authorized to charge to amount of \$ 505.00 to Deposit Account  
No. 02-2120 for payment of filing fees.

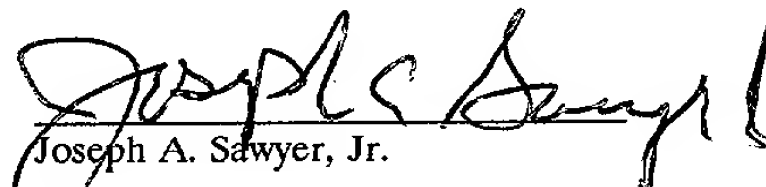
Respectfully submitted,

SAWYER & ASSOCIATES  
620 Hansen Way, Suite A  
Palo Alto, CA 94304  
(415) 493-4540

  
Joseph A. Sawyer, Jr.  
Attorney for Applicants  
Reg. No. 30,801

EXPRESS MAIL CERTIFICATE

I hereby certify that the above paper/fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on **July 28, 1997**, and is addressed to the Commissioner of Patents and Trademarks, Washington, DC 20231. "Express Mail" no.: EM548533254US.

  
Joseph A. Sawyer, Jr.

# **A METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT CARD TRANSACTION OVER THE INTERNET**

## **FIELD OF THE INVENTION**

The present invention relates generally to credit card transactions and specifically to detecting fraud in such credit card transactions when ordering and downloading information over the internet.

## **BACKGROUND OF THE INVENTION**

Credit card transactions are being utilized in a variety of environments. In a typical environment a user provides a merchant with a credit card, and the merchant through various means will verify whether that information is accurate. For example, referring now to Figure 1, a typical credit card verification system 10 is shown. In such a system, a merchant 12 receives a credit card from the customer 14. The merchant then verifies the credit card information through an automated verification system 16.

These systems work well in a credit card transaction in which either the customer has a face-to-face meeting with the merchant or the merchant is actually shipping a package or the like to the address of a customer. The verification procedure typically includes in the AVS system address information and identity information. However, when downloading information from an online service or the internet, the address and identity information is not enough for to adequately verify that the customer who is purchasing the goods is actually the owner of the credit card. For example, an individual may have both the name and the address of a

particular credit card holder and that information in a normal transaction may be sufficient for authorization of such a transaction. However, as an internet transaction it is possible to have all the correct information related to the particular credit card holder through unscrupulous means, and therefore, be able to fraudulently obtain information.

Accordingly, what is needed is a system and method that overcomes the problems associated with a typical verification systems for credit card transactions particularly in the internet or online services environment. The system should be easily implemented within the existing environment and should also be straightforwardly applied to existing technology. The present invention addresses such a need.

## SUMMARY

A method and system for detecting fraud in a credit card transaction between consumer and a merchant over the internet. The method and system comprises obtaining credit card information relating to the transaction from the consumer; and verifying the credit card information based upon a variety of parameters. The variety of parameters are weighted so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent. In so doing, an integrated verification system is provided which allows a merchant, or the like, to accurately and efficiently determine the validity of a transaction over the internet.

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is diagram of the prior art verification system for credit card transaction.

Figure 2 is a verification system in accordance with the present invention.

5 Figure 3 is a flow chart of the verification system in accordance with the present invention.

Figure 4 is a flow chart of the integrated verification system in accordance with the present invention.

## 10 DETAILED DESCRIPTION

The present invention relates to a fraud detection for use in credit card transaction over online services or the internet. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. Thus, the present invention is not intended to be limited to the embodiment shown but is to be accorded the widest scope consistent with the principles and features described herein.

20 The present invention provides an integrated verification system for credit cards transactions over an online service or the internet. Referring now to Figure 2, what is shown is a block diagram of a system 100 which would use the verification procedure in accordance with the present invention. System 100 includes similar to

Figure 1, a customer 102 and a merchant 104. The customer 102 provides the merchant with a credit card, the merchant then sends it to an integrated verification system IVS 106 which includes a variety of parameters providing consistency, history and other information in an integrated fashion to determine the credit card holder's validity. The IVS 106 is typically implemented in software for example in a hard disk, floppy disk or other computer-readable medium. In a typical embodiment, when the customer 102 orders a particular piece of software to be downloaded from a merchant 104, the merchant will provide the credit card number, e-mail address and other pertinent information to the IVS 106. The integrated verification system 106 then weights the variety of parameters so as to provide a merchant with a quantifiable indication on whether the credit and transaction is fraudulent. To more clearly describe the operation of a system and method in accordance with the present invention, refer now to the following discussion in conjunction with the accompanying figures.

Figure 3 shows a simple block diagram for providing an integrated verification of a credit card transaction over the internet. The IVS 106 includes a controller 212 which receives the credit information from the merchant and then sends that information on to a variety of parameters 202-208. The plurality of parameters that operate on the information to provide an indication of whether the transaction is valid. In this embodiment, the plurality of parameters comprises a history check 202, a consistency check 204, an automatic verification system 206 and an internet identification verification system 208. The output or individual indications of validity of these parameters are provided to fraud detector 210. The fraud detector 210

combines these inputs to provide an integrated indication of whether the particular transaction is valid.

Consistency check 204 allows one to determine whether the credit information is consistent, i.e., does the credit information match the user and other information. AVS system 206 provides similar information as AVS 16 described in Figure 1. A key feature of both the history database and the internet ID database is that they can be accessed and the information there within can be supplemented by a variety of other merchants and, therefore, information from those merchants is obtainable thereby.

History information check 202 is provided which also accesses a database 222 which may include card number and email information. The history check 202 will also actively determine if the particular transaction matches previous database information within the history database 222. Therefore, the internet ID verification system and history check increases in utility over time. The internet ID verification system 208 provides for a system for verifying the validity of an internet address, the details of which will be discussed hereinafter. The internet identification verification system similar to the history check includes a database 224 which can be added to by other merchants.

In addition, the internet identification verification system 208 accesses and communicates with a database of internet addresses. This system will be used to verify whether the internet address is consistent with other internet addresses being used in transactions utilizing this credit card.

These different parameters are weighted via weighting blocks 214-220,

respectively, dependent upon the particular credit card transaction. For example, if the amount of dollar transaction is critical, it may be appropriate for the history and AVS system 202 and 204 to be weighted more critically than the other parameters. On the other hand, if a critical point is the consistency of the internet address, then the consistency check 204 and the internet identification system 208 may be more critical. Accordingly, each of the verification parameters 202-208 may be weighted in different amounts depending upon its importance in the verification process.

A particularly important feature of the present invention is the internet identification system 208 and its operation within the integrated verification system 106. Through this system 208, it is possible to quickly determine if an internet identification address is being utilized fraudulently. To describe this feature in more detail, refer now to Figure 4 and the accompanying discussion.

Figure 4 is a flow chart of the internet identification verification system 208. The goal of internet identification verification system 208 is to determine whether the physical address or the physical location of the address compares to a previous physical location that was used for that particular internet address. Accordingly, in the flow chart of Figure 4, first the number of transactions that had been processed using that particular internet address is obtained from the database 224, via step 302. Thereafter, a map of those transactions is constructed based on those obtained transactions, via step 304. Finally, the constructed map is used to determine if the new credit card transaction is valid, via step 306. Accordingly, through a system and method in accordance with this system, an internet identification verification system is provided which can quickly and easily determine whether a particular internet



address is related to a particular credit care transaction.

Accordingly, what is provided is a system and method for accurately determining whether a particular credit card transaction is a fraudulent one. The integrated verification system in accordance with the present invention provides for weighting the variety of parameters so as to provide a merchant with a quantifiable indication on whether the credit and transaction is fraudulent.

Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will recognize that there could be variations to the embodiment and those variations would be within the spirit and scope of the present invention. Therefore, although the present invention was described in terms of a particular verification system, one of ordinary skill in the art readily recognizes, that any number of parameters can be utilized and their use would be within the spirit and scope of the present invention. Accordingly, many modifications may be made by one of ordinary skill without departing from the spirit and scope of the present invention, the scope of which is defined by the following claims.



## CLAIMS

What is claimed is:

1. A method for detecting fraud in a credit card transaction between consumer and a merchant over the internet comprising the steps of:

5 a) obtaining credit card information relating to the transaction from the consumer; and

b) verifying the credit card information based upon a plurality of parameters; the plurality of parameters being weighted so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

10 2. The method of claim 1 wherein the plurality of parameters include a consistency check, a history check, an automatic verification system and an internet identification system.

3. The method of claim 2 wherein the history check includes a database which can be accessed and supplemented by other merchants.

15 4. The method of claim 2 wherein the internet identification system includes a database which can be accessed and supplemented by other merchants.

5. An integrated verification system for determining credit card transactions between a merchant and consumer over the internet are fraudulent, the system comprising:

20 a controller for receiving credit card transaction information;

a plurality of parameters for receiving the transaction information from the controller means and for providing individual indications of the validity of transactions;

and detector means for receiving the indications of validity and providing an integrated indication of validity.

6. The system of claim 5 wherein each of the plurality of parameters includes a weighting factor.

5 7. The system of claim 5 wherein the plurality of parameters include a consistency check, a history check, an automatic verification system and an internet identification system.

8. The system of claim 7 wherein the history check includes a database which can be accessed and supplemented by other merchants.

10 9. The system of claim 7 wherein the internet identification system includes a database which can be accessed and supplemented by other merchants.

10. A method for verifying the validity of a credit card transaction over the internet comprising the steps of:

15 a) obtaining other transactions utilizing an internet address that is identified with the credit card transaction;

b) constructing a map of credit card numbers based upon the other transactions and;

c) utilizing mapped transactions to determine if the credit card transaction is valid.

20 11. A system for detecting fraud in a credit card transaction between consumer and a merchant over the internet comprising:

means for obtaining credit card information relating to the transaction from the consumer; and

means for verifying the credit card information based upon a plurality of parameters; the plurality of parameters being weighted so as to provide a merchant with a quantifiable indication of whether the credit care transaction is fraudulent.

5           12.    The system of claim 11 wherein the plurality of parameters include a consistency check, a history check, an automatic verification system and an internet identification system.

          13.    The system of claim 12 wherein the history check includes a database which can be accessed and supplemented by other merchants.

10           14.    The system of claim 12 wherein the internet identification system includes a database which can be accessed and supplemented by other merchants.

          15.    A computer readable containing program instructions for detecting fraud in a credit card transaction between consumer and a merchant over the internet, the program instructions:

15           a)    obtaining credit card information relating to the transaction from the consumer; and

          b)    verifying the credit card information based upon a plurality of parameters; the plurality of parameters being weighted so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

20           16.    A computer readable medium containing program instructions for verifying the validity of a credit card transaction over the internet, the program instructions:

          a)    obtaining other transactions utilizing an internet address that is

identified with the credit card transaction;

b) constructing a map of credit card numbers based upon the other transactions and;

c) utilizing mapped transactions to determine if the credit card transaction is valid.

5

10

10

5

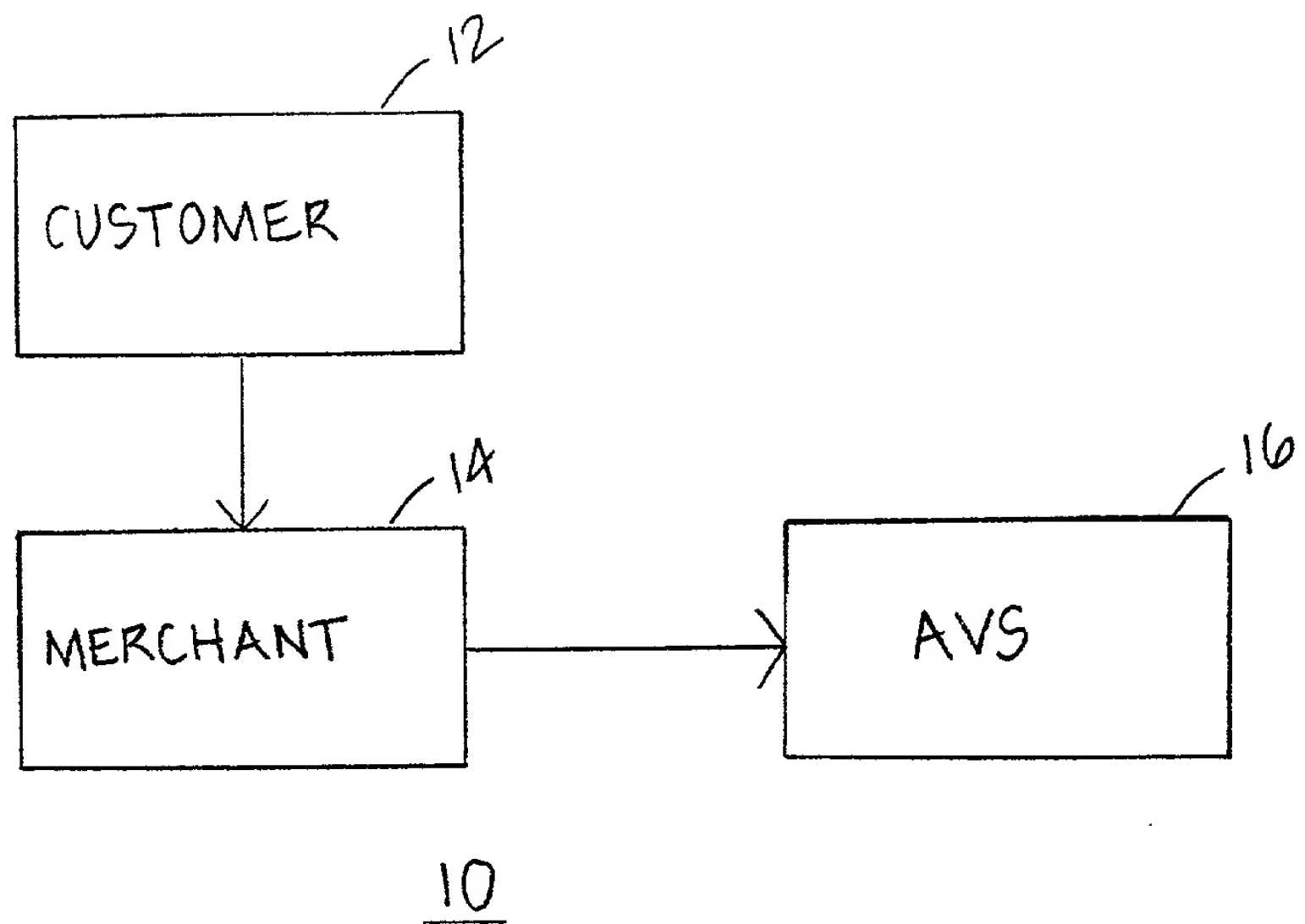


FIG. 1

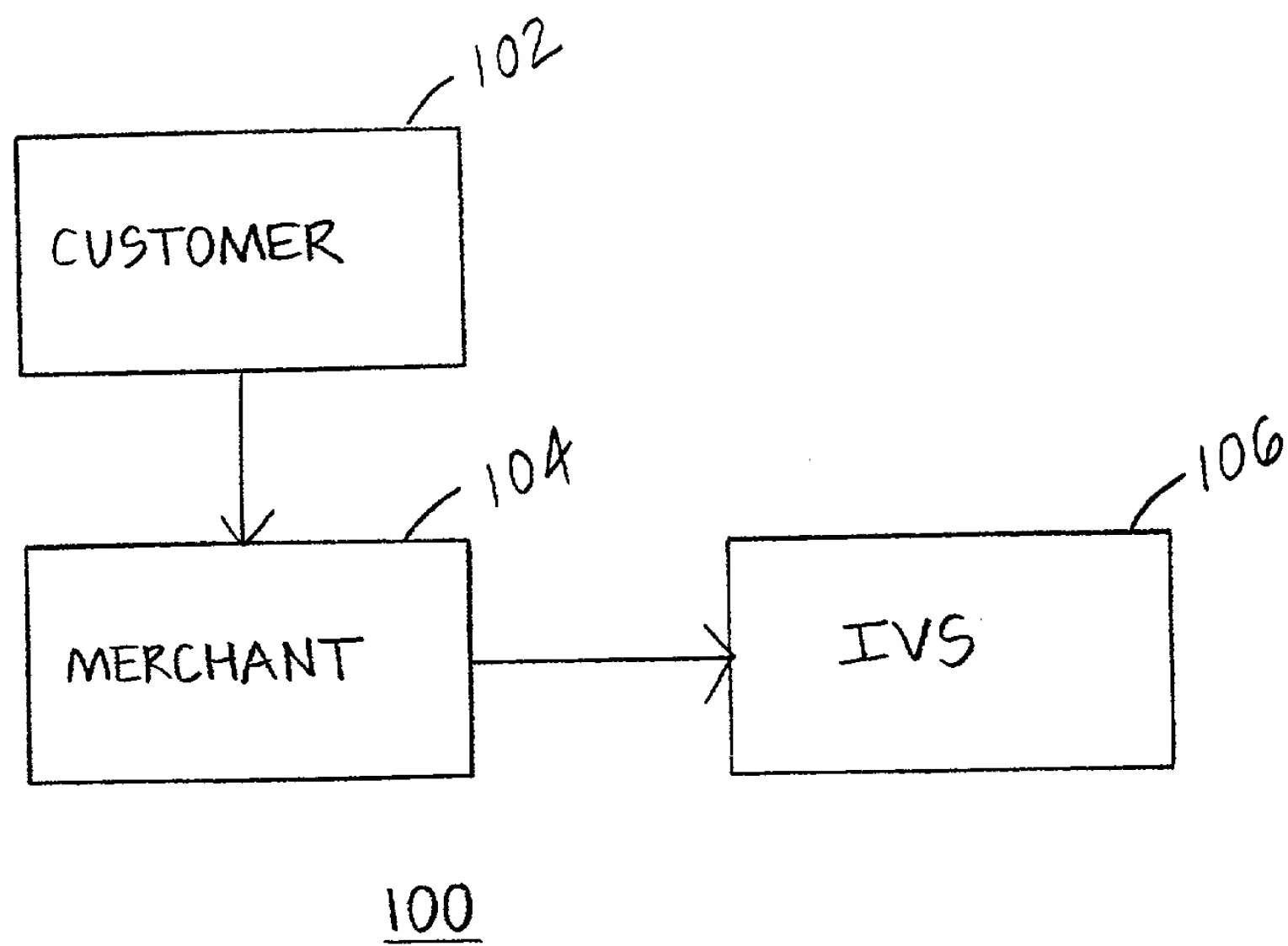


FIG. 2



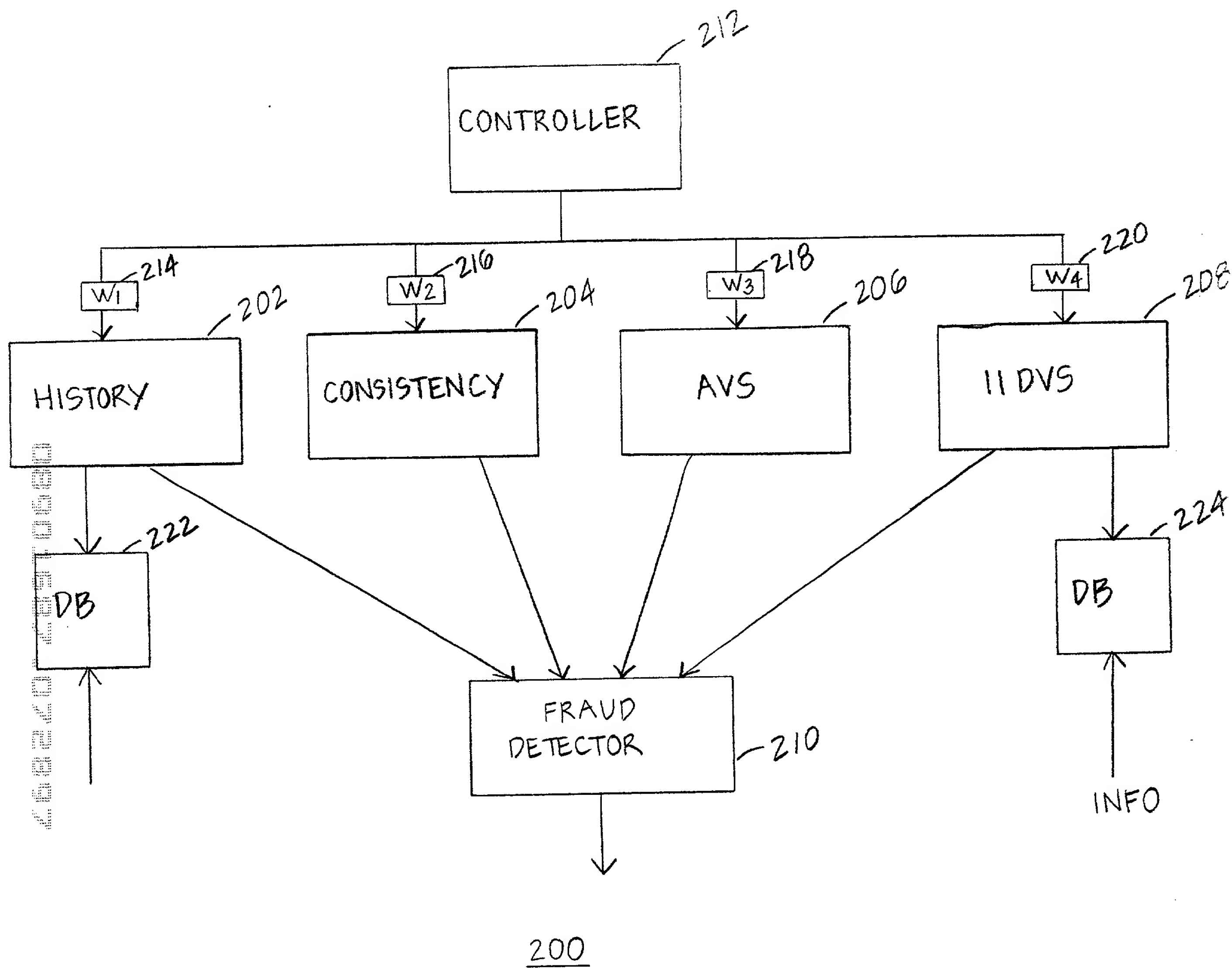


FIG. 3

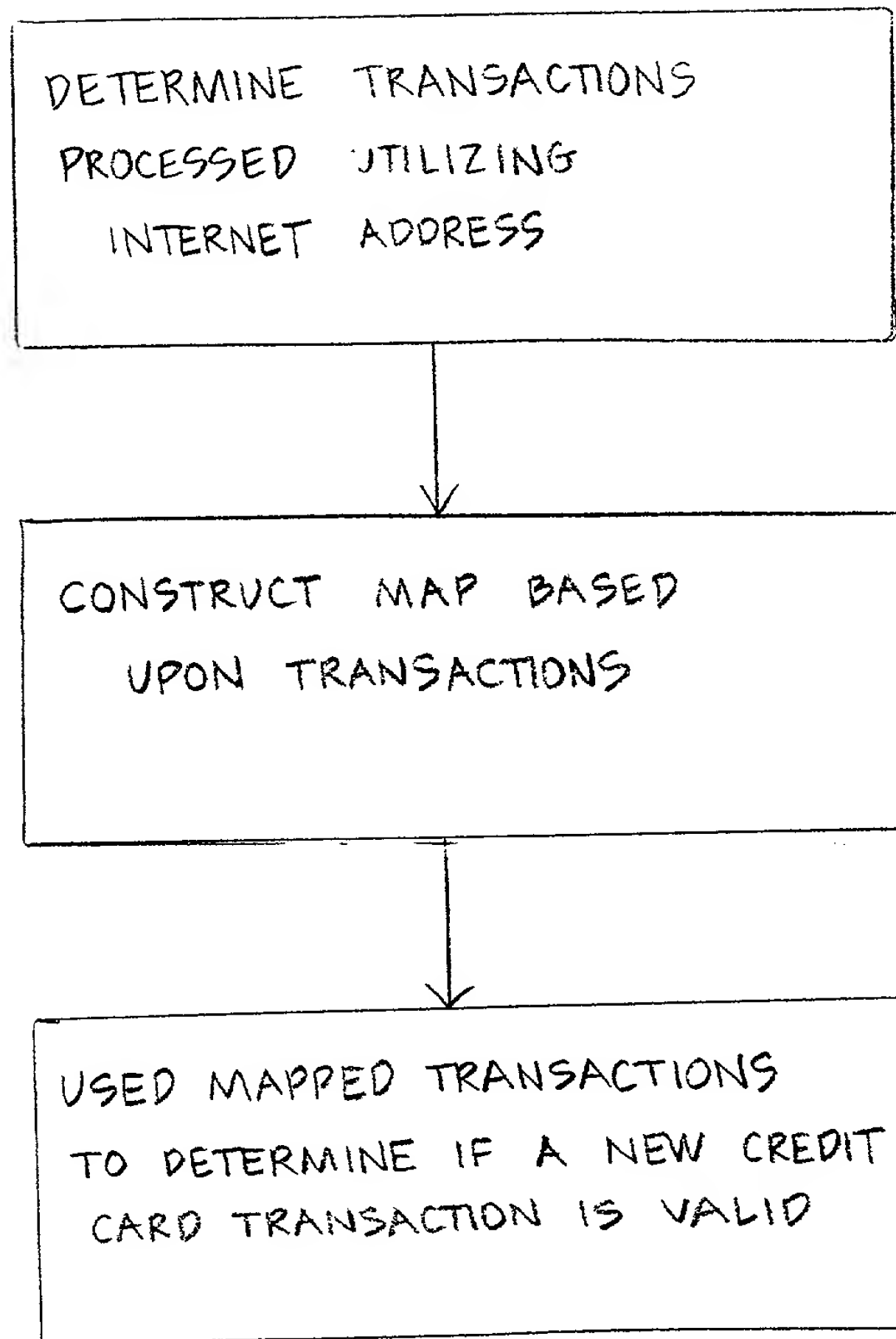


FIG. 4

DECLARATION

As the below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; and that I verily believe I am the original, first and sole inventor of the invention entitled:

**A METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT CARD TRANSACTION OVER THE INTERNET**

described and claimed in the specification which is attached hereto that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above; that I do not know and do not believe the same was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months prior to this application, that I acknowledge my duty to disclose information of which I am aware which is material to the examination of this application, and that no application for patent or inventor's certificate on said invention has been filed in any country foreign to the United States of America by me or my legal representatives or assigns.

Address all telephone calls to Mr. Sawyer at telephone number (415) 493-4540 and all correspondence to:

**Joseph A. Sawyer Jr.  
SAWYER & ASSOCIATES  
620 Hansen Way, Suite A  
Palo Alto, California 94304**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of sole or


First Inventor: **John Philip Pettitt**

Residence: **650 Palm Avenue  
Los Altos, California 94022**

Post Office Address: **650 Palm Avenue  
Los Altos Santa Clara CA 94022  
City County State Zip**

Citizenship: **U.K.**

7/24/97  
Date

  
Signature

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of: John Philip Pettitt

Title: A METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT  
CARD TRANSACTION OVER THE INTERNET

POWER OF ATTORNEY BY ASSIGNEE  
AND EXCLUSION OF INVENTOR UNDER 37 C.F.R. §1.32

Box Patent Application  
Washington, D.C. 20231

Sir:

Cybersource Corporation, a corporation organized and existing under and by virtue of the laws of the State of California, having become the owner of all rights in and to the above-identified application by virtue of an Assignment executed by the inventors concurrently with the execution of the application, said Assignment being submitted herewith for recording, hereby appoints:

Joseph A. Sawyer, Jr., Reg. No. 30,801  
Janyce R. Mitchell, Reg. No. 40,095

whose address is:

SAWYER & ASSOCIATES  
620 Hansen Way, Suite A  
Palo Alto, California 94304

as their attorney, to prosecute said application and to transact in connection therewith all business in the Patent and Trademark Office and before competent International Authorities; said appointment to be to the exclusion of the inventor and his attorneys in accordance with the provisions of 37 C.F.R. §1.32.

7/24/97  
Date

W.S. McKiernan  
William S. McKiernan  
President and  
Chief Executive Officer

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: )  
 )  
 John Philip Pettitt )  
 )  
 Serial No. )  
 )  
 Filed: Herewith )  
 )  
 For: A METHOD AND SYSTEM FOR )  
 DETECTING FRAUD IN A CREDIT )  
 CARD TRANSACTION OVER THE )  
 INTERNET )

**DECLARATION CLAIMING SMALL ENTITY  
 STATUS UNDER 37 CFR 1.9(f) and 1.27(c)  
 SMALL BUSINESS CONCERN**

I hereby declare that I am

☐ the owner of the small business concern identified below:

☒ an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN Cybersource Corporation  
 ADDRESS OF CONCERN 550 South Winchester Boulevard, Suite 301  
San Jose, CA 95128-2545

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.3-18, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal years, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention entitled A METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT CARD TRANSACTION OVER THE INTERNET by inventor John Philip Pettitt described in the application filed herewith.

The rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights to the invention is listed below\* and no rights to the invention are held by any person, other than the inventor, who could not qualify as a small business concern under 37 CFR 1.9(d) or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

\*NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this declaration is directed.

NAME OF PERSON SIGNING:

William S. McKiernan

TITLE OF PERSON OTHER THAN OWNER:

President and Chief Executive Officer

ADDRESS OF PERSON SIGNING:

550 South Winchester Boulevard, Suite 301

San Jose, CA 95128-2545

W. S. McKiernan

Signature

7/25/97

Date